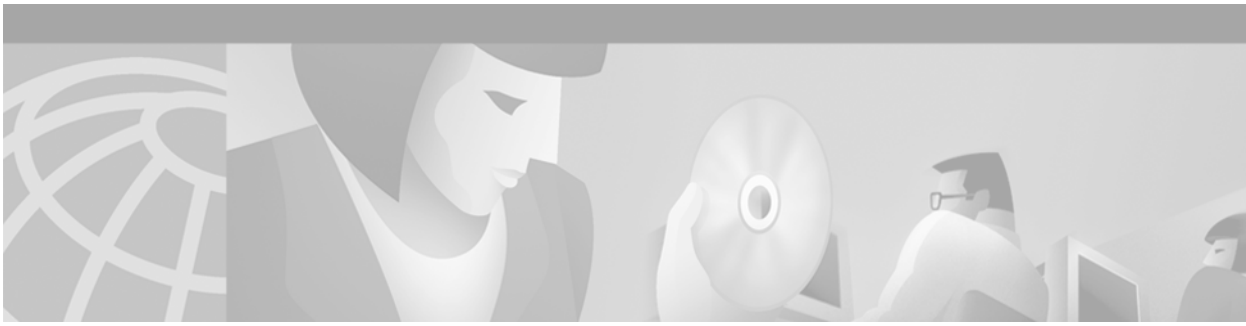


Cisco 3660 Modular Access Router with AIM-VPN/BP Security Policy

Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Cisco 3660 router. This security policy describes how the Cisco 3660 router meets the security requirements of FIPS 140-1, and how to operate the Cisco 3660 router in a secure FIPS 140-1 mode. This policy was prepared as part of the Level 2 FIPS 140-1 certification of the Cisco 3660 router.

Note This document may be copied in its entirety and without modification. All copies must include the copyright notice and statements on the last page.

FIPS 140-1 (Federal Information Processing Standards Publication 140-1 - Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-1 standard and validation program is available on the NIST website at the following NIST website:

http://csrc.nist.gov/cryptval/

This document contains the following sections:

- Introduction, page 1
- Cisco 3660 Modular Access Routers, page 2
- Secure Operation of the Cisco 3660 Router, page 13
- Network Modules and WAN Interface Cards, page 15
- Tables of Supported Cards, page 16
- Obtaining Documentation, page 19
- Obtaining Technical Assistance, page 21

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2001. Cisco Systems, Inc. All rights reserved.

References

This document deals only with operations and capabilities of the Cisco 3660 router in the technical terms of a FIPS 140-1 cryptographic module security policy. More information is available on the Cisco 3660 router and the entire 3600 Series from the following sources:

- The Cisco Systems website contains information on the full line of Cisco Systems products. Refer to the following website:

  http://www.cisco.com

- The 3600 Series product descriptions can be found at the following website:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3600/3600hig/3600ovr.htm

- For answers to technical or sales related questions, please refer to the contacts listed on the following website:

  http://www.cisco.com

Terminology

In this document, the Cisco 3660 router is referred to as the router, the module, or the system.

Document Organization

The Security Policy document is part of the complete FIPS 140-1 Submission Package. In addition to this document, the complete Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Module Software Listing
- Other supporting documentation as additional references

This document provides an overview of the Cisco 3660 router and explains the secure configuration and operation of the module. This introduction section is followed by the Cisco 3660 Modular Access Routers section, which details the general features and functionality of the Cisco 3660 router. The Secure Operation of the Cisco 3660 Router sectionspecifically addresses the required configuration for the FIPS-mode of operation.

This Security Policy and other Certification Submission Documentation was produced by Corsec Security, Inc. under contract to Cisco Systems. With the exception of this Non-Proprietary Security Policy, the FIPS 140-1 Certification Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

Cisco 3660 Modular Access Routers

The Cisco 3660 series multiservice platform improves on the density, performance, robustness and serviceability of the very successful Cisco 2600 and 3600 series family of products, extending these capabilities for use in larger branch-office applications or for telco-managed services as customer premise equipment (CPE). The Cisco 3660 series offers one or two autosensing 10/100 Ethernet ports

on the motherboard, six network module slots, two Advanced Interface Module (AIM) slots, an integrated power supply with optional redundancy, one console port, one AUX port, and two personal computer memory card international association (PCMCIA) card slots.

The additional slots of the Cisco 3660 series combined with the increased capabilities of new network modules enable new business applications, such as higher densities of packetized voice aggregation and branch-office Asynchronous Transfer Mode (ATM) access ranging from T1/E1 Inverse Multiplexing for ATM (IMA) to OC-3 interfaces. With over 70 different interfaces available today, the Cisco 3660 series provides unprecedented versatility, unmatched functionality and extensive flexibility with a variety of configurable options for customer-specific applications.

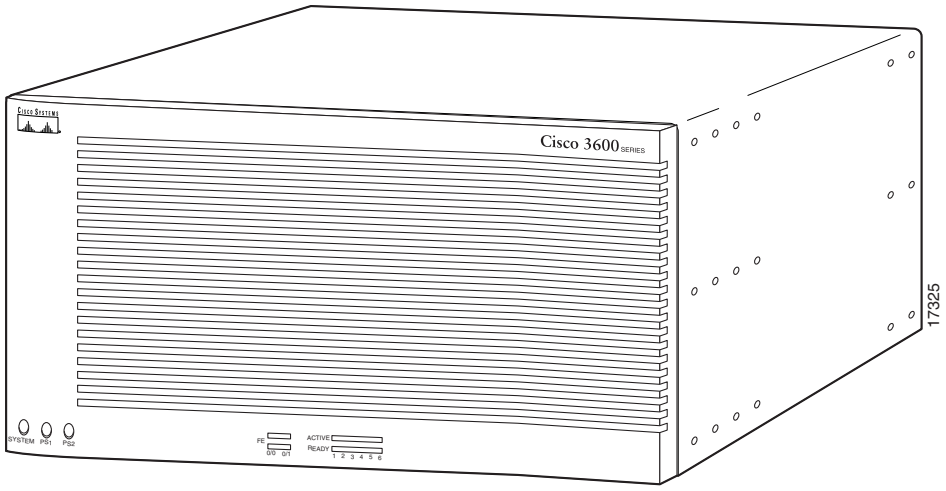
The Cisco 3660 series shares modular interfaces with the Cisco 1600, 1700, 2600, and 3600 series multiservice platforms, thereby protecting customer investment, streamlining operations costs associated with sparing of parts, and simplifying training. The modular chassis of the Cisco 3660 series is designed with high availability and serviceability in mind, making it a robust yet highly cost-effective element in the network over which to deploy mission-critical applications. Distinguishing features of the Cisco 3660 series include optional integrated power redundancy, and module hot-swap capabilities, which provide higher product availability for critical functions.

The Cisco 3660 Cryptographic Module

The metal casing that fully encloses the module establishes the cryptographic boundary for the router, all the functionality discussed in this document is provided by components within the casing. Cisco IOS features such as tunneling, data encryption, and termination of Remote Access WANs via IPSec, Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocols (L2TP) make the Cisco 3600 an ideal platform for building virtual private networks or outsourced dial solutions. Cisco 3600`s RISC-based processor provides the power needed for the dynamic requirements of the remote branch office, achieving wire speed Ethernet to Ethernet routing with up to 25 thousand packets per second (Kpps) throughput capacity.

Figure 1 shows a Cisco 3660 modular access router.

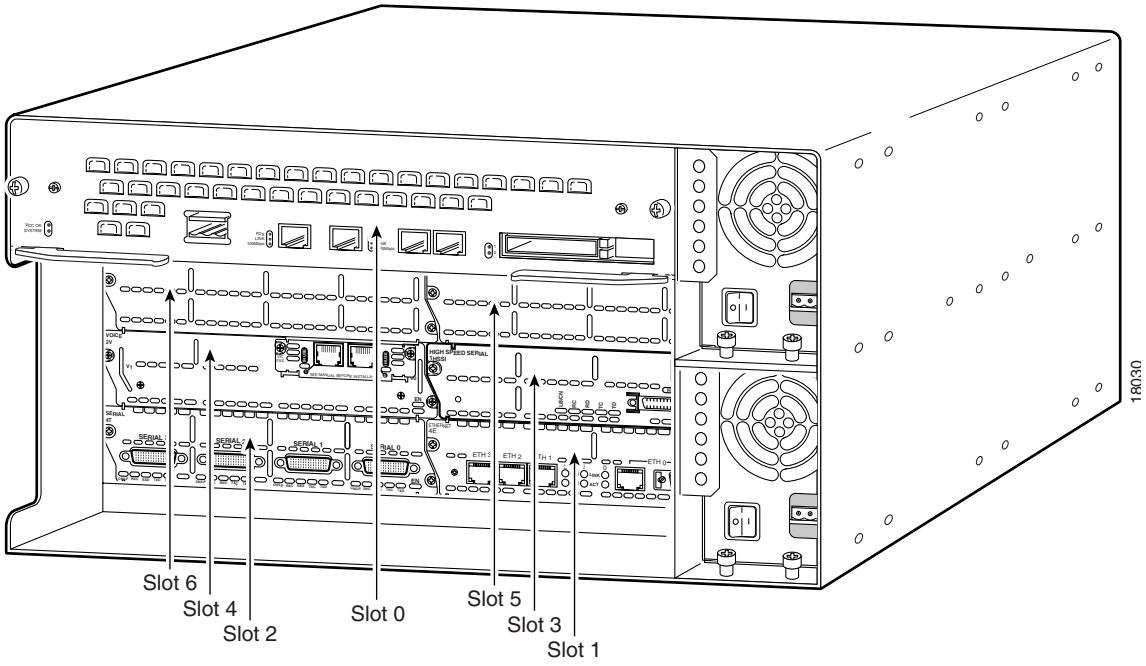
Figure 1 Cisco 3660 Router



Module Interfaces

The interfaces for the router are located on the rear panel as shown in Figure 2.

Figure 2 Physical Interfaces



The physical interfaces include power plug for the power supply and a power switch. The router has two Fast Ethernet (10/100 RJ-45) connectors for data transfers in and out. The module also has two other RJ-45 connectors on the back panel for a console terminal for local system access and an auxiliary port for remote system access or dial backup using a modem. The 10/100Base-T LAN ports have Link/Activity, 10/100Mbps, and half/full duplex LEDs. Figure 4 shows the LEDs located on the rear panel with descriptions detailed in Table 1:

Figure 3 Rear Panel LEDs

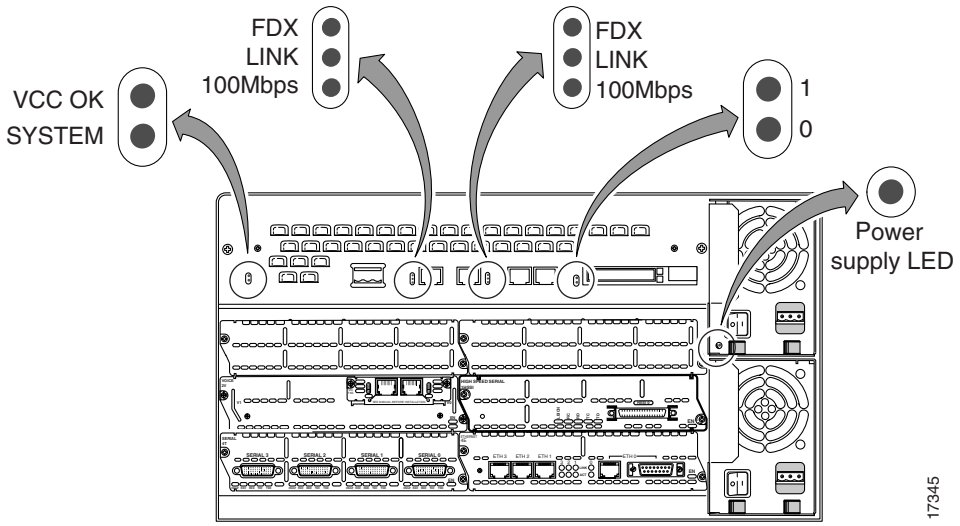
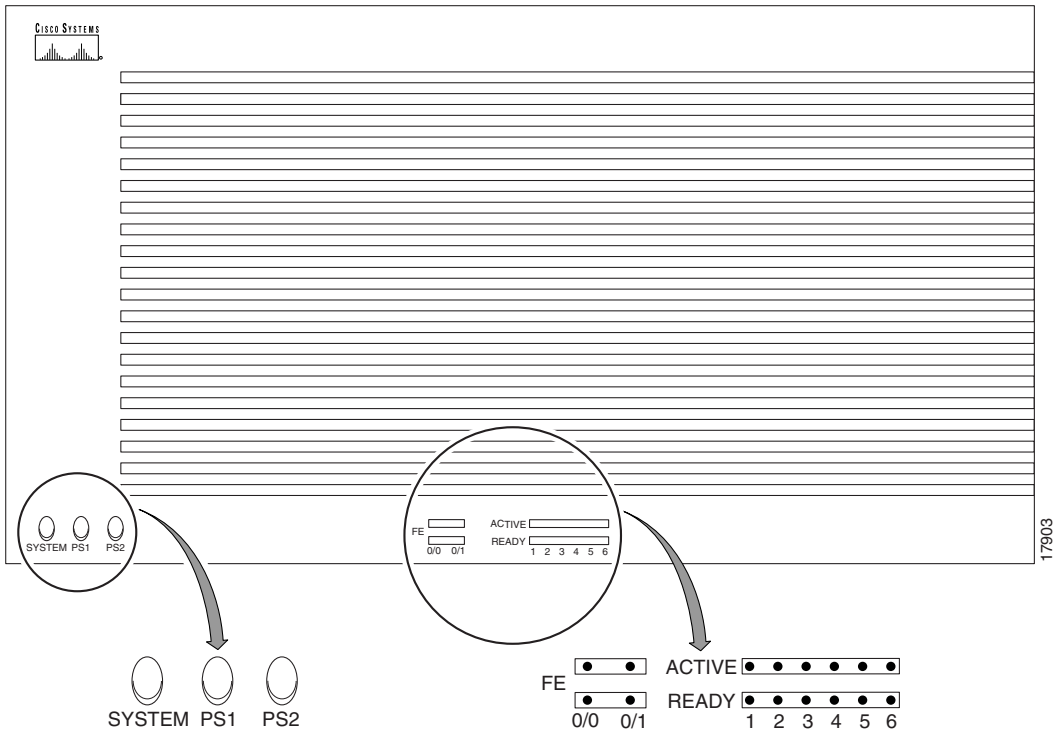


Table 1 Rear Panel LEDs and Descriptions

LED	Indication	Description
Power	Green	Operating voltages on the mainboard are within acceptable ranges
	Off	An error condition is detected in the operating voltages
System	Solid Green	Power is supplied to the router and the router is operational.
	Off	The router is not powered on.
	Blinking Green	Router is running the ROM monitor. No errors detected.
	Amber	Router is receiving power but not functioning properly. Possible power-on self-test error or over-temperature condition detected.
	Alternating Green/Amber	Power-on self-test detected. The router is attempting to reload the ROM monitor.
LINK	Green	An Ethernet link has been established
	Off	No Ethernet link established
FDX	Green	The interface is transmitting data in full-duplex mode
	Off	When off, the interface is transmitting data in half-duplex mode
100 Mbps	Green	The speed of the interface is 100 Mbps
	Off	The speed of the interface is 10 Mbps or no link is established
PCMCIA 0, 1	Green	Indicates data activity on the respective PCMCIA slot.

Figure 4 shows the front panel LEDs, which provide overall status of the router's operation. The front panel displays whether or not the router is booted, if the redundant power is (successfully) attached and operational, and overall activity/link status.

Figure 4 Front Panel LEDs



The following table provides more detailed information conveyed by the LEDs on the front panel of the router:

Table 2 Front Panel LEDs and Descriptions

LED	Indication	Description
System	Off	The router is not powered on.
	Blinking Green	Router is running the ROM monitor. No errors detected.
	Solid Green	Power is supplied to the router and the router is operational.
	Amber	Router is receiving power but not functioning properly. Possible power-on self-test error or over-temperature condition detected.
	Alternating Green/Amber	Power-on self-test detected. The router is attempting to reload the ROM monitor.

Table 2 Front Panel LEDs and Descriptions

LED	Indication	Description
PS1	Off	Power off or failed.
	Green	Installed and operating correctly.
	Blinking Amber	Thermal or out-of-range voltage protection shutdown.
	Amber	Installed with fault condition(s) detected.
PS2	Off	Power off or failed.
	Green	Installed and operating correctly.
	Blinking Amber	Thermal or out-of-range voltage protection shutdown.
	Amber	Installed with fault condition(s) detected.
ACTIVE 0, 1, 2, 3	Blinking Green	Indicates network activity on the module installed in the indicated slot.
READY 0, 1, 2, 3	Blinking Green	Functional module has been installed in the indicated slot
	Off	The slot is empty or the module is not functional.
FE 0/0 Active	Blinking Green	Indicates network activity on the Fast Ethernet 0/0 interface
FE 0/1 Active	Blinking Green	Indicates network activity on the Fast Ethernet 0/1 interface
FE 0/0 Ready	Green	Fast Ethernet interface 0/0 is functional.
FE 0/1 Ready	Green	Fast Ethernet interface 0/1 is functional.

All of these physical interfaces are separated into the logical interfaces from FIPS as described in the following table:

Table 3 FIPS 140-1 Logical Interfaces

Router Physical Interface	FIPS 140-1 Logical Interface
10/100BASE-TX LAN Port WAN Interface Network Module Interface Console Port Auxiliary Port* PCMCIA slot*	Data Input Interface
10/100BASE-TX LAN Port WAN Interface Network Module Interface Console Port Auxiliary Port* PCMCIA slot*	Data Output Interface
Power Switch Console Port Auxiliary Port*	Control Input Interface
10/100BASE-TX LAN Port LEDs System Power LED PS1/PS2 LEDs Fast Ethernet Active LED Fast Ethernet Ready LED Network Module Active LED Network Module Ready LED Power LED PCMCIA LEDs Console Port Auxiliary Port*	Status Output Interface
Power Plug	Power Interface

*The auxiliary port must be disabled in FIPS mode. See the Secure Operation of the Cisco 3660 Router section.

In addition to the built-in interfaces, the router also has approximately 70 network modules that can optionally be placed in an available slot. These networks modules have many embodiments, including multiple Ethernet, token ring, and modem cards to handle frame relay, ATM, and ISDN connections. See the "Network Modules and WAN Interface Cards" section on page 15 for a more detailed description of network modules and how they apply to the FIPS certification.

Roles and Services

There are two main roles in the router (as required by FIPS 140-1) that operators may assume: Crypto Officer role and User role. The administrator of the router assumes the Crypto Officer role in order to configure and maintain the router using Crypto Officer services, while the Users exercise only the basic User services.

Crypto Officer Services

During initial configuration of the router a Crypto Officer or Administrator password is defined and all management services are available from this role. The Administrator connects to the router through the console port via terminal program. An administrator of the router may assign permission to access the Administrator role to additional accounts, thereby creating additional administrators.

At the highest level, Crypto Officer services include the following:

- Configure the router: define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, load authentication information, etc.
- Define Rules and Filters: create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
- Status Functions: view the router configuration, routing tables, active sessions, use Gets to view SNMP MIB II statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status
- Manage the router: log off users, shutdown or reload the router, manually back up router configurations, view complete configurations, manager user rights, restore router configurations, etc.
- Set Encryption/Bypass: set up the configuration tables for IP tunneling. Set keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.
- Change Network Modules: insert and remove modules in the network module slot as described in Physical Security, page 10 of this document.
- Change WAN Interface Cards: insert and remove modules in the network module slot as described in Physical Security, page 10 of this document.

A complete description of all the management and configuration capabilities of the Cisco 3660 router can be found in the Performing Basic System Management manual and in the online help for the router.

User Services

A User enters the system by accessing the console port with a terminal program. The IOS prompts the User for their password. If it matches the plaintext password stored in IOS memory, the User is allowed entry to the IOS executive program. The services available to the User role include:

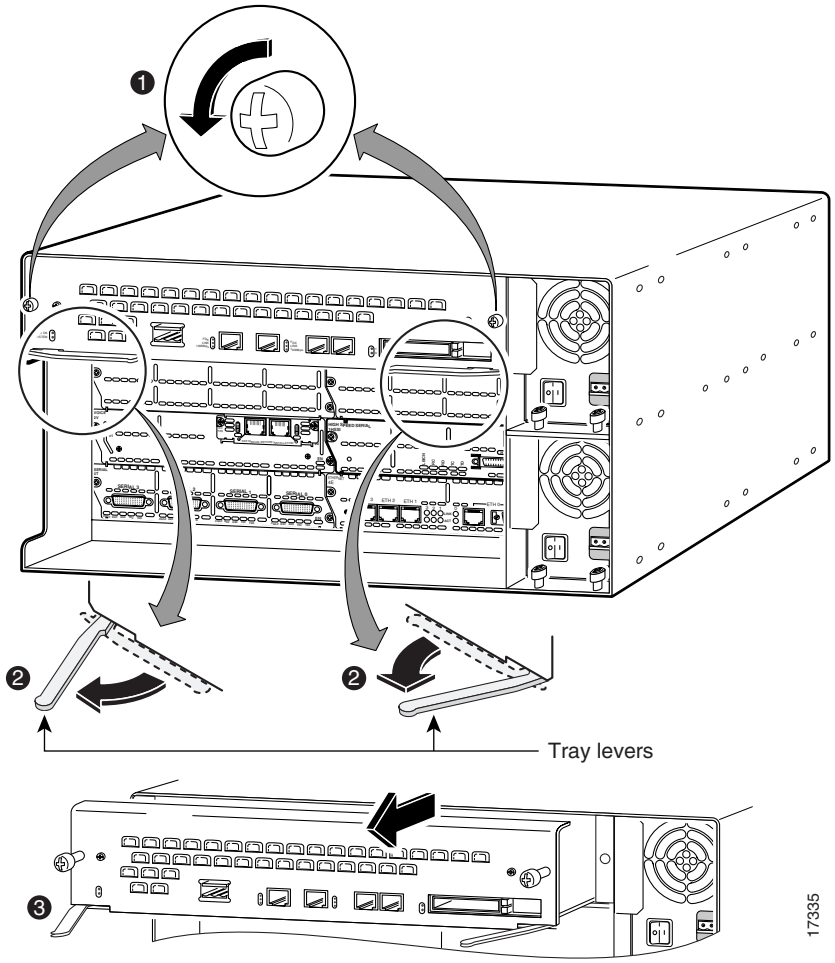
At the highest level, User services include the following:

- Status Functions: view state of interfaces, state of layer 2 protocols, version of IOS currently running
- Network Functions: connect to other network devices through outgoing telnet, PPP, etc. and initiate diagnostic network services (i.e., ping, mtrace)
- Terminal Functions: adjust the terminal session (e.g., lock the terminal, adjust flow control)
- Directory Services: display directory of files kept in flash memory

Physical Security

The router is entirely encased by a thick steel chassis. The rear of the unit provides 1 Network Module slot, 2 WIC slots, on-board LAN connectors, Console/Auxiliary connectors, the power cable connection and a power switch. The top portion of the chassis may be removed (see Figure 5) to allow access to the motherboard, memory, expansion slots and Advanced Interface Module.

Figure 5 Chassis Removal



Once the router has been configured in to meet FIPS 140-1 Level 2 requirements, the router cannot be accessed without signs of tampering. To seal the system, apply serialized tamper-evidence labels as follows:

Step 1 Clean the cover of any grease, dirt, or oil before applying the tamper evidence labels. Alcohol-based cleaning pads are recommended for this purpose. The temperature of the router should be above 10ºC.

Step 2 The tamper evidence label should be placed so that the one half of the tamper evidence label covers the enclosure and the other half covers the front panel of the router.

Step 3 The tamper evidence label should be placed so that the one half of the label covers the enclosure and the other half covers the Cisco 3660 mainboard.

Step 4 The tamper evidence label should be placed over the PCMCIA Flash card slots.

Step 5 The tamper evidence label should be placed so that the one half of the label covers the enclosure and the other half covers the Network Module Slot 1.

Step 6 The tamper evidence label should be placed so that the one half of the label covers the enclosure and the other half covers the Network Module Slot 2.

Step 7 The tamper evidence label should be placed so that the one half of the label covers the enclosure and the other half covers the Network Module Slot 3.

Step 8 The tamper evidence label should be placed so that the one half of the label covers the enclosure and the other half covers the Network Module Slot 4.

Step 9 The tamper evidence label should be placed so that the one half of the label covers the enclosure and the other half covers the Network Module Slot 5.

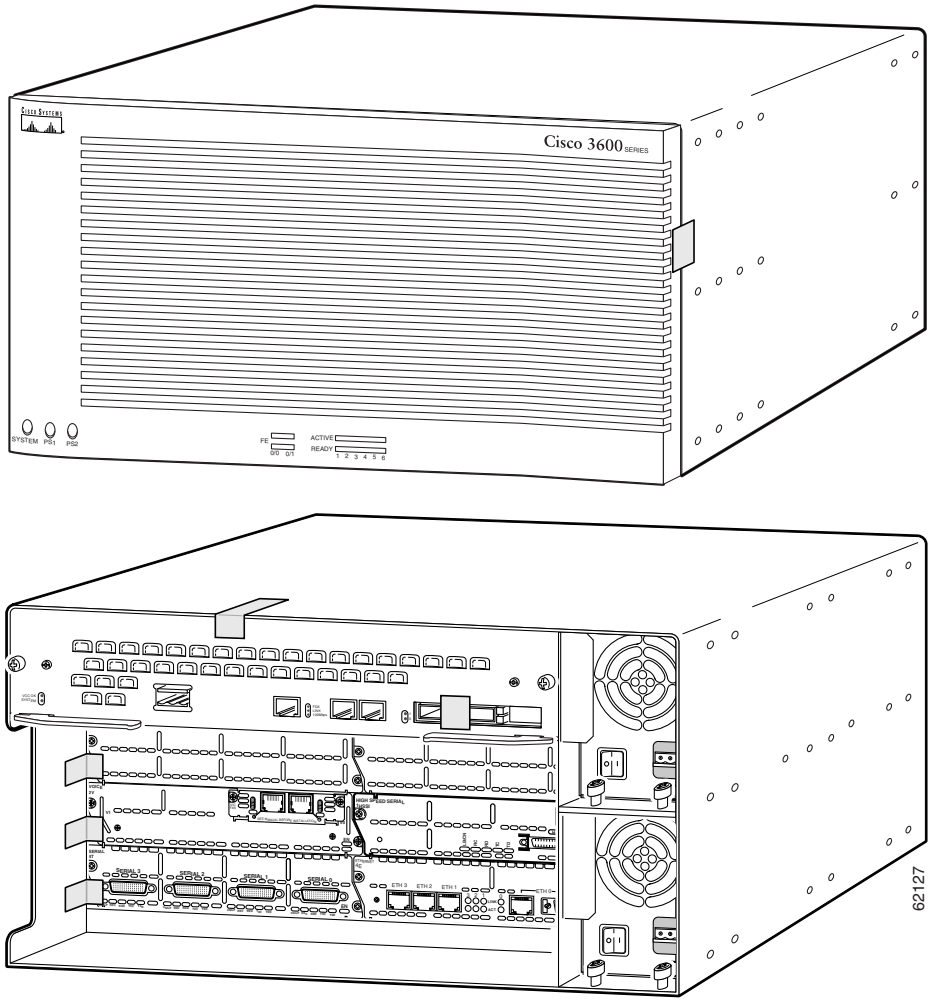
Step 10 The tamper evidence label should be placed so that the one half of the label covers the enclosure and the other half covers the Network Module Slot 6.

Step 11 The tamper evidence label should be placed so that the half of the label covers the enclosure and the other half covers the WAN interface card slot. Any attempt to remove a WAN interface card will leave tamper evidence.

Step 12 If applicable, place a label such that it covers both the daughter WAN interface cards on the mixed-media LAN/Network Module. Any attempt to remove a WAN interface card will show tamper evidence.

Step 13 The labels completely cure within five minutes.

Figure 6 Tamper-Evident Labels



The tamper evidence seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the router, remove network modules or WIC cards, or the front faceplate will damage the tamper evidence seals or the painted surface and metal of the module cover. Since the tamper evidence labels have non-repeated serial numbers, the labels may be inspected for damage and compared against the applied serial numbers to verify that the module has not been tampered. Tamper evidence labels can also be inspected for signs of tampering, which include the following: curled corners, bubbling, crinkling, rips, tears, and slices. The word "Opened" may appear if the label was peeled back.

Cryptographic Key Management

The router securely administers both cryptographic keys and other critical security parameters such as passwords. The tamper evidence seals provide physical protection for all keys. Keys are also password protected and can be zeroized by the Crypto Officer. Keys are exchanged manually and entered electronically via manual key exchange or Internet Key Exchange (IKE).

The Cisco 3660 router contains a cryptographic accelerator card, which provides DES (56-bit) and 3DES (168-bit) IPSec encryption at up to 32Mbps (3DES, 96Mbps DES), MD5 and SHA-1 hashing, and has hardware support for DH, RSA, and DSA key generation.

Self-Tests

In order to prevent any secure data being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The router includes an array of self-tests that are run during startup and periodically during operations. The self-test run at power-up includes a cryptographic known answer tests (KAT) on the FIPS-approved cryptographic algorithms (DES, 3DES), on the message digest (SHA-1) and on Diffie-Hellman algorithm. Also performed at startup are software integrity test using an EDC, and a set of Statistical Random Number Generator (RNG) tests. The following tests are also run periodically or conditionally: a Bypass Mode test performed conditionally prior to executing IPSec, a software load test for upgrades and the continuous random number generator test. If any of these self-tests fail, the router will transition into an error state. Within the error state, all secure data transmission is halted and the router outputs status information indicating the failure.

Secure Operation of the Cisco 3660 Router

The Cisco 3660 router meets all the Level 2 requirements for FIPS 140-1. Follow the setting instructions provided below to place the module in FIPS mode. Operating this router without maintaining the following settings will remove the module from the FIPS approved mode of operation.

Initial Setup

Step 1 The Crypto Officer must apply tamper evidence labels as described in the Physical Security section of this document. The Crypto Officer must securely store tamper evidence labels before use, and any tamper evidence labels not used should also be stored securely.

Step 2 Only a Crypto Officer may add and remove network modules. When removing the tamper evidence label, the Crypto Officer should remove the entire label from the router and clean the cover of any grease, dirt, or oil with an alcohol-based cleaning pad. The Crypto Officer must re-apply tamper evidence labels on the router as described in the Physical Security section.

Step 3 Only a Crypto Officer may add and remove WAN Interface Cards. When removing the tamper evidence label, the Crypto Officer should remove the entire label from the router and clean the cover of any grease, dirt, or oil with an alcohol-based cleaning pad. The Crypto Officer must re-apply tamper evidence labels on the router as described in the Physical Security section.

System Initialization and Configuration

Step 1 The Crypto Officer must perform the initial configuration. The IOS version shipped with the router, version 12.1(5)T, is the only allowable image. No other image may be loaded.

Step 2 The value of the boot field must be 0x0101 (the factory default). This setting disables break from the console to the ROM monitor and automatically and boots the IOS image. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

```
config-register 0x0101
```

Step 3 The Crypto Officer must create the "enable" password for the Crypto Officer role. The password must be at least 8 characters and is entered when the Crypto Officer first engages the "enable" command. The Crypto Officer enters the following syntax at the "#" prompt:

```
enable secret [PASSWORD]
```

Step 4 The Crypto Officer must always assign passwords (of at least 8 characters) to users. Identification and authentication of the console port is required for Users. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

```
line con 0
password [PASSWORD]
login local
```

Step 5 The Crypto Officer shall only assign users to a privilege level 1 (the default).

Step 6 The Crypto Officer shall not assign a command to any privilege level other than its default.

Step 7 The PCMCIA Flash memory card slot is not configured in FIPS mode. Its use is restricted via tamper evedence labels (see the Physical Security section).

Non-FIPS Approved Algorithms

The following algorithms are not FIPS approved and should be disabled:

- RSA for encryption
- MD-4 and MD-5 for signing
- ah-sha-hmac
- esp-sha-hmac
- HMAC SHA-1

Protocols

The following network services affect the security data items and must not be configured: NTP, TACACS+, RADIUS, Kerberos.

SNMP v3 over a secure IPSec tunnel may be employed for authenticated, secure SNMP gets and sets. Since SNMP v2C uses community strings for authentication, only gets are allowed under SNMP v2C.

Remote Access

Auxiliary terminal services must be disabled, except for the console. The following configuration disables login services on the auxiliary console line.

```
line aux 0
no exec
```

Telnet access to the module is only allowed via a secure IPSec tunnel between the remote system and the module. The Crypto officer must configure the module so that any remote connections via telnet are secured through IPSec.

Network Modules and WAN Interface Cards

With over 70 modular interface options, the Cisco 3660 provides solutions for data, voice, video, hybrid dial access, virtual private networks (VPNs), and multi-protocol data routing. The high-performance, modular architecture protects customers' investment in network technology and integrates the functions of several devices into a single, manageable solution.

Each network module and WAN Interface Card (WIC) meets FIPS 140-1 requirements for physical interfaces. They are classified as data input interfaces and data output interfaces. Network modules and WICs are an external interface, similar to the 100Base-T LAN ports. They expand the router's physical interfaces with multi-port ATM modules, multi-port Ethernet modules, high-speed serial interfaces, etc. A list all network modules and WICs is included with this document (see theTables of Supported Cards section).

Network Modules

When a network module is inserted, it fits into an adapter called the network module expansion bus. The expansion bus interacts with the PCI bridge in the same way that the fixed LAN ports do; therefore, no critical security parameters pass through the network module (just as they don't pass through the LAN ports).

The Cisco 3660 block diagram clearly depicts the distinction between the network module slot and the AIM socket. The block diagram for the crypto card clearly delineates that the network modules and network module expansion bus have no direct interaction with the crypto card. Therefore, no security parameters pass through the network module expansion bus to the crypto card or vice versa.

The expansion bus for the network module card is inside the cryptographic boundary, but it services only the network modules (physical interfaces) and has no effect on the cryptographic processing of the module. If the expansion bus were at the router's cryptographic boundary (as opposed to being inside the boundary), the same principles would apply. While the cryptographic boundary is drawn at the router case, adding and removing network modules will not compromise the security of the router.

As described in the Roles and Services section, only a Crypto Officer may replace a network module. If someone other than the Crypto Officer attempts to change a network module, the stickers over the network module slot will indicate tamper evidence. Thus, only valid network modules will be used and only the proper authority may change them. The Roles and Services section provides instructions to change network modules in a FIPS-approved manner.

WAN Interface Cards

WICs are similar to network modules in that they greatly increase the router's flexibility. The WICs are inserted into one of two slots, which are located above the fixed LAN ports. WICs interface directly with the processor. They do not interface with the cryptographic card; therefore no security parameters will pass through them. WICs cannot perform cryptographic functions; they only serve as a data input and data output physical interface. Please refer to the block diagrams for further reference. Only the Crypto Officer may change WICs, and they must follow the same guidelines for changing network modules (see the Roles and Services section).

Console Port

Additionally, the console port does not directly interface with the network modules or the WICs; therefore, no critical security parameters will be passed over the network modules, WICs, or cryptographic processing card from the terminal.

Conclusion

Network modules and WAN Interface Cards do not affect the cryptographic processing of the router, nor are they privy to any security parameters contained in the router's cryptographic card. The following table describes the input data types and output data types of network modules and WICs:

Network Module and WAN Interface Card	
Input Data type	**Output Data type**
Plaintext data that is to be encrypted from the local area network	Plaintext data that has been decrypted by the module
Encrypted input from the remote modules (Wide Area Network)	Ciphertext data that has been encrypted by the module
Internet Key Exchange information from the remote module	Internet Key Exchange information from the module
Status information	

No critical security parameters are passed though either of these interfaces. These interfaces do not perform any cryptographic functions, and "hot swapping" these interfaces by the Crypto Officer as described in the "Initial Setup" section on page 13 does not compromise the security of the router.

Tables of Supported Cards

Network Modules

Serial Network Modules

NM-16A	16 port high-density async network module
NM-32A	32 port high-density async network module
NM-4T	Four-port serial network module
NM-4A/S	Four-port async/sync serial network module
NM-8A/S	Eight-port async/sync serial network module

LAN Network Modules and Mixed-Media LAN/WAN Network Modules

NM-1FE-TX	One-port Fast Ethernet network module (10/100BaseTX only)
NM-1FE-FX	One-port Fast Ethernet network module (10/100Base Fiber only)
NM-4E	Four-port Ethernet network module
NM-1E	One-port Ethernet network module
NM-1E2W	One-port Ethernet two WAN card slot network module
NM-2E2W	Two-port Ethernet two WAN card slot network module
NM-1E1R2W	One-port Ethernet one-port Token Ring two WAN card slot network module

ISDN and Channelized Serial Network Modules

NM-1CT1	One-port channelized T1/ISDN PRI network module
NM-1CT1-CSU	One-port channelized T1/ISDN PRI with CSU network module
NM-2CT1	Two-port channelized T1/ISDN PRI network module
NM-2CT1-CSU	Two-port channelized T1/ISDN PRI with CSU network module
NM-1CE1B	One-port channelized E1/ISDN PRI balanced network module
NM-1CE1U	One-port channelized E1/ISDN PRI unbalanced network module
NM-2CE1B	Two-port channelized E1/ISDN PRI balanced network module
NM-2CE1U	Two-port channelized E1/ISDN PRI unbalanced network module
NM-1FE1CT1	One-port Fast Ethernet and 1-port Channelized T1/ISDN-PRI network module
NM-1FE1CT1-CSU	One-port Fast Ethernet and 1-port Channelized T1/ISDN-PRI network module with integrated CSU
NM-2FE1CT1	One-port Fast Ethernet and 2-port Channelized T1/ISDN-PRI network module
NM-2FE1CT1-CSU	One-port Fast Ethernet and 2-port Channelized T1/ISDN-PRI network module with integrated CSU's
NM-1FE1CE1U	One-port Fast Ethernet and 1-port Channelized E1/ISDN-PRI network module
NM-1FE1CE1B	One-port Fast Ethernet and 1-port Channelized E1/ISDN-PRI network module
NM-1FE2CE1U	One-port Fast Ethernet and 2-port Channelized E1/ISDN-PRI network module
NM-1FE2CE1B	One-port Fast Ethernet and 2-port Channelized E1/ISDN-PRI network module
NM-4B-S/T	Four-port ISDN BRI network module
NM-4B-U	Four-port ISDN BRI with NT-1 network module

NM-1CT1	One-port channelized T1/ISDN PRI network module
NM-8B-S/T	Eight-port ISDN BRI network module (S/T Interface)
NM-8B-U	Eight-port ISDN BRI with NT-1 network module (U Interface)

Modem Modules

NM-8AM	Eight-port Analog Modem network module
NM-8AM-J	Eight-port Analog Modem network module for Japan
NM-16AM	16-port Analog Modem network module
NM-16AM-J	16-port Analog Modem network module for Japan
NM-6DM	Six digital modem network module
NM-12DM	12 digital modem network module
NM-18DM	18 digital modem network module
NM-24DM	24 digital modem network module
NM-30DM	30 digital modem network module
MICA-6MOD=	Six digital modem upgrade card

Voice/Fax Network Modules

NM-1V	One-slot Voice and Fax network module
NM-2V	Two-slot Voice and Fax network module

ATM Network Modules

NM-1ATM-25	One-port 25-Mbps ATM network module
NM-1A-OC3MM	One-port 155-Mbps OC-3 ATM multimode network modules
NM-1A-OC3SMI	One-port 155-Mbps OC-3 ATM single-mode intermediate-reach network modules
NM-1A-OC3SML	One-port 155-Mbps OC-3 ATM single-mode long-reach network modules

Other

RPS	600W redundant power supply option
NM-COMPR	Compression network module

Cisco 3600 WAN Interface Cards

Serial WAN Interface Cards

WIC-1DSU-T1	One-port T1/fractional T1 with CSU/DSU
WIC-1T	One-port high speed serial
WIC-1DSU-56K4	One-port four-wire 56kbps with CSU/DSU

ISDN WAN Interface Cards

WIC-1B-S/T	One-port ISDN BRI
WIC-1B-U	One-port ISDN BRI with NT1

WAN interface cards are available as daughter cards to the mixed-media LAN/WAN network modules. Up to two WAN interface cards can be installed on a single, mixed-media LAN/WAN network module.

Cisco 3600 Voice Interface Cards

Voice Interface Cards

VIC-2FXS	No description available
VIC-2FXO	No description available
VIC-2E/M	No description available
VIC-2FXO-M3	Two-port Voice Interface card- FXO (for Australia)
VIC-2FXO-EU	Two-port Voice Interface card- FXO (for Europe)
VIC-2BRI-S/T-TE	Two-port Voice Interface card- BRI (Terminal)

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the "References" section.

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, PIX, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

By printing or making a copy of this document, the user agrees to use this information for product evaluation purposes only. Sale of this information in whole or in part is not authorized by Cisco Systems.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0106R)

Copyright © 1999, Cisco Systems, Inc.
All rights reserved.